LINEAR FORMS IN $p-ADIC ELLIPTIC LOGARITHMS (Analytic Number Theory and Surrounding Areas)

AUTHOR(S):

Hirata-Kohno, Noriko

数理解析研究所講究録 1384 巻 2004 年 72-79

LINEAR FORMS IN p-ADIC ELLIPTIC LOGARITHMS

p進楕円対数一次形式について

NORIKO HIRATA-KOHNO 平田典子

Department of Mathematics 日本大学理工学部数学科
College of Science and Technology
Nihon University
Suruga-Dai, Kanda
Chiyoda, Tokyo 101-8308, Japan
hirata@math.cst.nihon-u.ac.jp

Abstract

The aim of this article is to give an estimate of linear forms in p-adic logarithms in elliptic case. We define for this estimate a p-adic elliptic logarithmic function viewed as a local reversed function of the Lutz-Weil p-adic elliptic function. We also present some Taylor expansion estimates by means of formal groups of elliptic curves, which would be useful to describe arithmetical behaviors of the function.

1. Introduction

Let K be an algebraic number field of finite degree D over the rational number field $\mathbb{Q}$. Consider $\mathcal{E}$ an elliptic curve defined over K, which is defined by the Weierstraß equation of the following form: $y^2 = x^3 - ax - b \quad (a, b \in O_K)$ with $4a^3 \neq 27b^2$.

Let $|\cdot|$ be an Archimedean valuation on K and p be a rational prime $\in \mathbb{Q}$. For a place v of K over p, we write the valuation $|\cdot|_v$ normalized such that $|x|_v = p^{-ord_p(x)}$ for $x \in \mathbb{Q}$. Denote K_v the completion of K by v, and write $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ by p. The field K_v is a finite extention of $\mathbb{Q}_p$ of local degree $d_v = [K_v : \mathbb{Q}_p]$. Put $\mathbb{C}_p$ the completion of the algebraic closure of K_v (we note that the algebraic closure of K_v is not complete). We know that $\mathbb{C}_p$

is algebraically closed complete field of charasteristic 0, in which the algebraic closure of K_v is dense and that there are D distinct embeddings of K into $\mathbb{C}_p$.

Put $\lambda_p = \frac{1}{p-1}$ if $p \neq 2$, and $\lambda_2 = 3$. We set $\mathcal{C}_p := \{z \in \mathbb{C}_p : |z|_v < p^{-\lambda_p}\}$ and $\mathcal{C}_v := \mathcal{C}_p \cap K_v$. Let $\beta_1, \cdots, \beta_k \in K$ with $|\beta_i|_v \leq 1$ for any i, $1 \leq i \leq k$.

2. p-adic elliptic function

We recall the definition of the Lutz-Weil elliptic p-adic function. It is known that there exists an analytic function φ defined on $\mathcal{C}_v \to K_v$, satisfying $\varphi(0) = 0$, $\varphi'(0) = 1$ and the differential equation $(Y')^2 = 1 - aY^4 - bY^6$. We may also enlarge the domain of the definition of this function φ to $\mathcal{C}_p$. For the p-adic Lie-group $\mathcal{E}(\mathbb{C}_p)$ we have the exponential map $\mathcal{C}_p \to \mathcal{E}(\mathbb{C}_p)$ represented by

$$\exp_p(z) = \left(\varphi(z), \varphi'(z), \varphi^3(z)\right)$$

which is called the Lutz-Weil elliptic p-adic function.

Thus the elliptic curve is written by $Y^2Z = X^3 - aXZ^2 - bZ^3$ for $(X, Y, Z) = (\varphi, \varphi', \varphi^3)$. The difference between this p-adic exponential map and the complex one is the fact that φ is locally analytic only on $\mathcal{C}_p$, not on $\mathbb{C}_p$. Indeed, φ is an odd and injective function such that $|\varphi(z)|_v = |z|_v$, $|\varphi'(z)|_v = 1$ for any $z \in \mathcal{C}_p$, then $\exp_p$ has no period. There are corresponding addition formula and derivation formula like the Weierstraß elliptic function $\wp$.

For an algebraic number, write $h(\cdot)$ as the absolute logarithmic projective height.

3. Our p-adic lower bound

Now we present our estimate of linear forms in p-adic logarithms in elliptic case.

Main Theorem *Let $\mathcal{E}_1 \cdots, \mathcal{E}_k$ be elliptic curves defined by $y^2 = x^3 - a_i x - b_i$ where $a_i, b_i \in O_K$ $(1 \leq i \leq k)$. Put*

$$h = \max_{1 \leq i \leq k} \{h(1, a_i, b_i), 1\}.$$

For $1 \leq i \leq k$, let

$$0 \neq u_i \in \{u \in \mathcal{C}_v : \exp_p(u) \in \mathcal{E}_i(K)\}.$$

Define $U_i = \dfrac{p^{-\lambda_p}}{|u_i|_v}$ (> 1) *and* V_i *by*

$$\log V_i \geq \max\{h(\exp_p(u_i)), \frac{1}{D}\} \quad (1 \leq i \leq k)$$

where we may suppose

$$U_1 = \max(U_i),\ V_1 = \max(V_i), \quad 1 \leq i \leq k.$$

Let $\beta_1, \cdots \beta_k \in K - \{0\}$, $\quad |\beta_i|_v \leq 1\,(1 \leq i \leq k)$ *and put*

$$\log B \geq \max_{1 \leq i \leq k}{}^{\bullet}\{1, h(\beta_i)\}.$$

If $\beta_1 u_1 + \cdots + \beta_k u_k \neq 0$, *then there exists an effective constant* $C > 0$ *depending only on* k, p *such that*

$$\log |\beta_1 u_1 + \cdots \beta_k u_k|_v \geq$$

$$-C \cdot D^{2k+2}\,(\log B + h + \log\log V_1 + \log DU_1)$$

$$\times\,(\log\log V_1 + h + \log DU_1)^{k+1} \times \prod_{i=1}^{k}(h + \log V_i + \log U_i)$$

(these log*'s mean the usual Archimedean logarithms).*

4. p-adic elliptic logarithmic function

The proof of the theorem relies on the usual transcendence machine which is also settled in p-adic elliptic case (*see* [Be] [R-U]), as well as p-adic case of usual logarithmic function (*see* [Yu1] [Yu2]) except our following new point.

Let us present our definition of p-adic elliptic logarithmic function. It is just defined below as a local reversed function of our injective $\exp_p(z)$ around the origin, but in practice, since we need everywhere explicit estimates, we define the function by using the formal group of elliptic curve. We thus have explicit estimates deduced from Taylor expansion of $\exp_p(z)$ and see that the n-th Taylor coefficient of p-adic elliptic logarithmic function at the origin has the denominator $2n$, that is indeed analogous to the usual Archimedean logarithmic function having the denominator n (*see* [Da-Hi1] [Da-Hi2]).

Let us recall the formal group of the elliptic curves as follows. Let us consider the equation $y^2 = 4x^3 - ax - b$ (we may slightly modify the equation by 4).

We below introduce a local parameter t and define $w(t)$. We see $t \sim z$ around $z = 0$. This t is a local uniformizer at the origin of the elliptic curve, and leads to consider a power series ring in one variable t on $\mathcal{E}$. In fact, in Archimedean case, it is already known that $w(t)$ is a formal power series in t (Proposition 1.1 (a), Page 111 of [Sil]) and an estimate is given by David and the author [Da-Hi2]. We note below that the series has a positive radius of convergence around the origin, namely $w(t)$ can be identified with its Taylor series. We denote by $z = z(t) = \int \Omega(t)$, where $\Omega(t)$ is a differential form in the local parameter t (*see* [Sil], Chapter IV, Section 5), then by this $z(t)$ we have in Lemma 2 our definition of an elliptic logarithmic function in p-adic case.

Here we present explicit estimates.

Lemma 1 *Consider the elliptic curve defined by*

$$y^2 = 4x^3 - ax - b, \quad a, b \in K.$$

Let $t = -\dfrac{2x}{y}$, $\quad w(t) = -\dfrac{2}{y}$, $\quad \alpha = -\dfrac{a}{4}$, $\quad \beta = -\dfrac{b}{4}$. *Then we have*

$$w(t) = \sum_{k \geq 3} A_n t^n$$

with

$$A_n = \sum_{4p+6q=n-3, p,q \in \mathbb{Z}, p,q \geq 0} a_{p,q}^{(n)} \alpha^p \beta^q \quad (n \geq 3)$$

where $a_{p,q}^{(n)} \in \mathbb{Z}$ *with*

$$|a_{p,q}^{(n)}| \leq \frac{3^3 \cdot 8^{n-3}}{n^3 (p+1)^3 (q+1)^3} \quad (n \geq 3, p \geq 0, q \geq 0).$$

Moreover, we have

$$h(A_n) \leq 5n + nh.$$

Outline of the proof of Lemma 1 It is known that the coefficient A_n is written in a homogeneous polynomial of degree $n - 3$ (*see* Proposition 1.1, Chap 4 of [Sil]). We put $A = \alpha t (w(t))^2$ and $B = \beta (w(t))^3$. Then we get $w(t) = t^3 + A + B$ with

$$A = \sum_{n \geq 7} t^n \sum_{i_1 + i_2 = n-1} \sum_{4p_1 + 6q_1 = i_1 - 3} \sum_{4p_2 + 6q_2 = i_2 - 3} a_{p_1,q_1}^{(i_1)} a_{p_2,q_2}^{(i_2)} \alpha^{p_1 + p_2 + 1} \beta^{q_1 + q_2}$$

and $B =$

$$\sum_{n\geq 9} t^n \sum_{i_3+i_4+i_5=n} \sum_{j=3}^{5} \sum_{4p_j+6q_j=i_j-3} a^{(i_3)}_{p_3,q_3} a^{(i_4)}_{p_4,q_4} a^{(i_5)}_{p_5,q_5} \alpha^{p_3+p_4+p_5} \beta^{q_3+q_4+q_5+1}.$$

We have by induction :

$$|a^{(n)}_{p,q}| \leq \frac{3^3 \cdot 8^{n-3}}{n^3(p+1)^3(q+1)^3} \quad (4p+6q=n-3)$$

by means of $\displaystyle\sum_{i_1+i_2=n, i_1\geq 3, i_2\geq 3} \frac{1}{i_1^3 i_2^3} < \frac{1}{n^3}$ $(n \in \mathbb{Z}, n \geq 6)$.

To get the estimate the height of A_n, first we use $h(a^{(n)}_{p,q}) \leq n \log 8$ for any integers p, q with $4p+6q = n-3$ since

$$|a^{(n)}_{p,q}| \leq \frac{3^3 \cdot 8^{n-3}}{n^3(p+1)^3(q+1)^3} \leq 8^n.$$

Consider any place v satisfying $|A_n| > 1$. The cardinality of such places is finite. If v is an infinite place, we have

$$|A_n|_v = \left| \sum_{4p+6q=n-3, p,q\in\mathbb{Z}, p,q\geq 0} a^{(n)}_{p,q} \alpha^p \beta^q \right|_v$$

$$\leq \sum_{4p+6q=n-3, p,q\in\mathbb{Z}, p,q\geq 0} |a^{(n)}_{p,q}|_v |\alpha|_v^p |\beta|_v^q \leq 8^n \times \sum_{4p+6q=n-3, p,q\in\mathbb{Z}, p,q\geq 0} |\alpha|_v^p |\beta|_v^q$$

$$\leq 8^n (n-2) \max\{1, |\alpha|_v, |\beta|_v\}^{n-3}.$$

If v is a finite place, noting the fact $a^{(n)}_{p,q} \in \mathbb{Z}$, we have

$$|A_n|_v \leq \max_{4p+6q=n-3} |a^{(n)}_{p,q} \alpha^p \beta^q|_v \leq \max_{4p+6q=n-3} |\alpha^p \beta^q|_v \leq \max\{1, |\alpha|_v, |\beta|_v\}^{n-3}.$$

Then we obtain the estimate of $h(A_n)$ by definition of height and definition of α, β. □

The following statement gives the definition of our p-adic elliptic logarithmic function, showing that the n-th Taylor coefficient of the function has the denominator $2n$.

Lemma 2 *For x, y satisfying $y^2 = 4x^3 - ax - b \quad (a, b \in K)$, put $t = -\dfrac{2x}{y}$, $\quad w(t) = -\dfrac{2}{y}$, $\quad \alpha = -\dfrac{a}{4}$, $\quad \beta = -\dfrac{b}{4}$,*

$$\Omega(t) = \frac{dx}{y} = \frac{\frac{d}{dt}\left(\frac{t}{w(t)}\right)}{-\frac{2}{w(t)}}dt$$

and

$$z = z(t) := \int \Omega(t) = \int \frac{\frac{d}{dt}\left(\frac{t}{w(t)}\right)}{-\frac{2}{w(t)}}dt.$$

Then $z(t)$ is defined as a local reversed function of t namely an elliptic logarithmic function whose Taylor expansion is given by

$$z(t) = \sum_{n \geq 1} B_n t^n$$

with

$$B_n = -\frac{C_n}{2n}, \qquad C_n = \sum_{4p+6q=n-1, p,q \in \mathbb{Z}, p,q \geq 0} b_{p,q}^{(n)} \alpha^p \beta^q \quad (n \geq 1)$$

where $b_{p,q}^{(n)} \in \mathbb{Z}$ with

$$|b_{p,q}^{(n)}| \leq \frac{10^{4n}}{n^2(p+1)^3(q+1)^3} \quad (n \geq 1, p \geq 0, q \geq 0).$$

Moreover, we have

$$h(C_n) \leq 12n + nh.$$

Outline of the proof of Lemma 2 The function $z(t)$ is by definition an elliptic logarithmic function, namely the reversed function of $\varphi(z(t))$ around $t = 0$.

As $w(t)$ is reversible, put

$$\sum_{n \geq -3} D_n t^n = \frac{1}{w(t)} = \frac{1}{\sum_{n \geq 3} A_n t^n}.$$

We have $D_{-3} = 1$ and

$$\sum_{i+j=n} A_i D_j = 0 \quad (n \geq 1).$$

Suppose for $-3 \leq \nu \leq n-4$ that we have

$$D_n = \sum_{4p+6q=\nu+3} d_{p,q}^{(\nu)} \alpha^p \beta^q$$

with $d_{p,q}^{(\nu)} \in \mathbb{Z}$ and

$$|d_{p,q}^{(\nu)}| \leq \frac{10^{4(\nu+3)}}{(\nu+4)^3(p+1)^3(q+1)^3}$$

which is true for $\nu = -3$.

Using the relation above which implies $D_{n-3} = -(A_4 D_{n-4} + \cdots + A_{n+3} D_{-3})$, we get by induction hypothesis

$$|d_{p,q}^{(n-3)}| \leq \frac{10^{4n}}{(n+1)^3(p+1)^3(q+1)^3} .$$

We then obtain

$$z(t) = -\frac{1}{2} \int \sum_{n \geq 0} t^n \sum_{i+j=n, i \geq 3} (j+1) D_j A_i dt$$

$$= -\frac{1}{2n} \sum_{n \geq 1} t^n \sum_{i+j=n-1, i \geq 3} (j+1) D_j A_i .$$

Consequently, for $n \geq 1$ we obtain

$$\sum_{4p+6q=n-1} b_{p,q}^{(n)} \alpha^p \beta^q$$

$$= \sum_{i+j=n-1, i \geq 3} (j+1) \sum_{4p+6q=n-1} \alpha^p \beta^q \sum_{p_1+p_2=p, q_1+q_2=q} a_{p_1,q_1}^{(i)} d_{p_2,q_2}^{(j)} .$$

For $n = 1$,we have $b_{p,q}^{(n)} = b_{0,0}^{(1)} = -2$. Then the lemma is true. Suppose that this holds true for $n \geq 2$. Then the absolute value of the rational coefficient of $\alpha^p \beta^q$ above is bounded by

$$\frac{2^3 3^3 n 10^{4(n-1)}}{(n-1)^3(p+1)^3(q+1)^3} \leq \frac{10^{4n}}{n^2(p+1)^3(q+1)^3}$$

by means of the upper bound of $|d_{p,q}^{(n-3)}|$. Hence we obtain the upper bound of $|b_{p,q}^{(n)}|$.

The argument to estimate the height of A_n in Lemma 1 gives us the upper bound of $h(C_n)$. □

References

[Be] D. Bertrand, *Approximations diophantiennes p-adiques sur les courbes elliptiques admettant une multiplication complexe*, Compositio Math. 37 , no. 1 (1978), 21–50.

[Ch] G. V. Chudnovsky, *Contributions to the theory of transcendental numbers*, Amer. Math. Soc. Math. Surveys Monographs 19 (1984).

[Da] S. David, *Minorations de formes linéaires de logarithmes elliptiques*, Mémoires, Nouvelle série 62, Supplément au Bulletin de la Soc. Math. de France, Tome 123, Fascicule 3 (1995).

[Da-Hi1] S. David et N. Hirata-Kohno, *Recent progress on linear forms in elliptic logarithms*, in the Proceedings of the Conference "A Panorama in Number Theory", ed. by G. Wustholz, Cambridge University Press (2002), 26–37.

[Da-Hi2] S. David et N. Hirata-Kohno, *Linear Forms in Elliptic Logarithms*, preprint.

[La] S. Lang, *Elliptic functions*, Addison–Wesley (1973).

[Lu] E. Lutz, *Sur les approximations diophantiennes linéaires p-adiques*, Acutuallités scientifiques et industrielles 1224, Publ. de l'Institut de Math. de l'Université de Strasbourg XII, Hermann (1955).

[R-U] G. Re'mond et F. Urfels, *Approximation diophantienne de logarithmes elliptiques p-adiques*, J. Number Theory 57, no. 1 (1996), 133–169..

[Sil] J. H. Silverman, *The arithmetic of elliptic curves*, GTM 106 (Springer) (1986).

[Yu1] Kunrui Yu, *p-adic logarithmic forms and group varieties I*, J. Reine Angew. Math. 502 (1998), 29–92.

[Yu2] Kunrui Yu, *p-adic logarithmic forms and group varieties II*, Acta Arith. 89, no. 4 (1999), 337–378.